REMARKS

Claims 1, 3, 8-11, 24, 26, 28, 31, 36-39, 43, 48, 49, 50, 51 have been amended. No Claims have been cancelled. No Claims have been added. No new matter has been added as a result of these claim amendments. Claims 1 – 13, 24, 26, 28, and 30 – 53 remain under examination.

EXAMINER INTERVIEW SUMMARY

On September 21, 2006, Ronald Pomerenke, representative for the Applicants, conducted a telephonic interview with Examiner Eleni Shiferaw.

A proposed amendment to claim 1 that the Applicants FAXed to the Examiner was discussed. An additional proposed amendment to Claim 1, based on the second and third steps of Claim 3 was discussed. The Examiner indicated that if this amendment were submitted by the Applicants that the Examiner would enter the amendment.

ALLOWABLE SUBJECT MATTER

The Examiner has indicated that Claims 3, 31, and 43 are objected to as being dependent upon a rejected based claim, but would be allowable if re-written in independent form including all limitations of the base claims 1, 26, and 28 respectively and any intervening claims. Applicants thank the Examiner for indicating this allowable subject matter.

In the telephonic interview of September 21, 2006 Applicants discussed with the Examiner a proposed amendment to Claim 1 that would incorporate into Claim 1 some**, but**

not all, limitations from Claim 3. In particular, the Applicants proposed that the stricken language from Claim 3 presented below not be incorporated into Claim 1:

3. A method as recited in Claim 1, said step of determining a secret integer that is unique for the subset further comprising the steps of:

~~generating a first integer using a random number generator;~~

determining a shared secret key ~~to be shared with the receiving device~~ based on the first integer and a first public key associated with the receiving device; and

selecting the secret integer based on the shared secret key.

Applicants have amended Claim 1, as well as other independent claims, in accordance with this proposal. Applicants respectfully request entrance of this amendment, as per Applicants' agreement with the Examiner in the telephonic interview.

REJECTIONS BASED ON CITED ART

CLAIM REJECTIONS – 35 U.S.C. § 103

Claims 1-2, 4-13, 24, 26, 28, 30, 32-42, and 44 - 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hori et al. USPN 6,792,280 B1 in view of J. Franks et al. herein after Franks "An Extension to HTTP: Digest Access Authentication". The rejection to Claims 1-2, 4-13, 24, 26, 28, 30, 32-42,and 44 - 53 is respectfully traversed for the following reasons.

Claim 1 recites:

1. A method for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transfer protocol, the method comprising the computer-implemented steps of:

selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads, wherein determining the secret integer comprises:

determining a shared secret key based on a first integer and a first public key associated with a receiving device of the client and the server; and

selecting the secret integer based on the shared secret key;

encrypting the subset of data using at least the secret integer to generate encrypted data that is impractical for a device other than the client and the server to decrypt; and

sending, from a sending device of the client and the server to the receiving device, in the particular payload, the encrypted data and clue information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

Claim 1 has been amended by removing the words "machine-implemented" prior to "method." Applicants note that Claim 1 was filed and examined without the language machine-implemented. Applicants note that the Claim 1 was not rejected with respect to these limitations or lack thereof. Applicants had voluntarily added these limitations in a prior

response. However, Applicants assert that per *Ex parte Lundgren 76 USPQ 2d, 1385,* as well as other precedent, terms such as "machine-implemented" are not required in Claim 1.

For reasons already discussed, Applicants respectfully assert that currently amended Claim 1 is allowable over the prior art.

Applicants have amended Independent Claims 24, 26, 28 to recite similar limitations to those discussed in the response to Claim 1. For at least the reasons discussed in the response to Claim 1, Claims 24, 26, 28 are patentable.

DEPENDENT CLAIMS

Applicants have amended various dependent claims in order to conform the dependent claims with the amendment to the independent claims. For example, limitations from Claim 3 that were added to Claim 1, have been removed from Claim 3. With respect to Claims 8 – 10, the amendments are to maintain proper antecedent basis in view of the amendment to Claim 1.

Claims 2-13 depend from Independent Claim 1, incorporating limitations therefrom. As explained above, Claim 1 includes limitations that define patentable subject matter. Therefore, dependant Claims 2-13 recite patentable subject matter for at least the same reasons Claim 1 recites patentable subject matter. Furthermore, dependant Claims 2-13 recite additional limitations that further distinguish over the prior art.

Claims 30-53 depend from Independent Claims 26 or 28, incorporating limitations therefrom. As explained above, Claims 26 and 28 include limitations that define patentable

subject matter. Therefore, dependant Claims 30 -53 recite patentable subject matter for at least the same reasons Claims 26 and 28 recites patentable subject matter. Furthermore, dependant Claims 30 -53 recite additional limitations that further distinguish over the prior art.

CONCLUSION

The Applicants believe that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicants petition for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: October 4, 2006

Ronald M. Pomerenke
Reg. No. 43,009

2055 Gateway Place, #550
San Jose, CA 95110
Telephone: (408) 414-1080, ext. 210
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on Oct. 4, 2006 by Tracy Boylon